Examiner's Amendment

1. An extension of time under 37 CFR 1.136(a) is required in order to make an examiner's amendment which places this application in condition for allowance. During a telephone conversation conducted on 3/24/2010, Pehr Jannson, Reg. 35,759, requested an extension of time for 3 MONTH(S) and authorized the Director to charge Deposit Account No. 502114 the required fee of $1110.00 for this extension and authorized the following examiner's amendment. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

The application has been amended as follows:

Please cancel claim 2, add claim 17, and replace other claims with the following:

1. A method to secure the execution of at least one program in an electronic assembly comprising information processing means and information storage means, comprising

inserting directives, corresponding to beacons and beacon functions intended for a pre-processor, into the code of the program;

causing the pre-processor to replace at least one directive by a beacon determined to correspond to the directive, in the code of the program;

during the execution of said program, causing the electronic assembly to:

store one or more items of information concerning one or more characteristics of at least one beacon during the passage of said beacon and check, at~~,~~ at least one check point, the consistency of the information stored about all beacons encountered.

3. The method according to claim ~~2~~ 17, wherein the electronic ~~unit~~ assembly uses a control flow graph of the program to be protected to generate the static information used by the verification functions.

4. The method according to ~~claim 2~~ Claim 17 or 3, wherein a beacon is information which defines the characteristics of ~~the~~ a corresponding passage point and/or one or more other passage points.

5. The method according to claim 4, wherein the beacon is one of the following elements, a combination of several of them, or all of them:

an integer locating the beacon in the code to be protected;

a Boolean variable defining whether ~~it~~ the beacon is the first or the last beacon;

a data structure characterizing, according to the value of a register or a given variable, all beacons through which passage will be forbidden ~~(using a verification function)~~ in the remaining execution;

a data structure comprising, according to the value of a register or a given variable, all beacons through which passage will be forced ~~(using a verification function)~~ in the remaining execution.

6. The method according to ~~claims 2~~ Claim 17 or 3, wherein a beacon function is called by the program at each passage by a beacon and which consists in storing dynamically in a shared memory various items of information concerning the beacon.

7. The method according to claim 6, wherein the beacon function pushes the beacon onto a stack in the shared memory and/or one which updates a checksum contained in the shared memory with the beacon data.

8. The method according to one of ~~claims 2~~ Claim 17 or 3, further comprising calling a history verification function at each check point to check the consistency of the information stored in ~~the~~ a shared memory during the successive calls of the beacon functions.

9. An electronic assembly including information processing means and information storage means containing at least one program to be executed wherein the electronic assembly comprises:

the means required to insert directives, corresponding to beacons and beacon functions intended for a pre-processor, into the code of the at least one program;

the means required to cause the pre-processor to replace at least one directive by a beacon determined to correspond to the directive, in the code of the program;

the means required, during the execution of said program, and during the passage by at least one beacon, to store one or more items of information concerning one or more characteristics of said beacon in said storage means and means to check, at at least one check point, the consistency of the information stored about all beacons encountered.

11. A computer executable storage medium having a computer executable program code embodied therein, said computer executable program code adapted to be executed to secure the execution of at least one program in an electronic assembly having information processing

means and information storage means, said executable program code comprising instructions to direct a microprocessor of the electronic assembly to:

cause a pre-processor to replace at least one directive inserted into a program, the at least one directive corresponding to beacon and beacon functions, and intended for the pre-processor, by a determined beacon in the code of the program; and

during the execution of said program:

store one or more items of information concerning one or more characteristics of at least one beacon during the passage by said beacon and

check at, at least one check point, the consistency of the information stored about all beacons encountered.

12. A computer readable storage medium having a computer executable program code embodied therein, said computer executable program code adapted to be executed to secure the execution of at least one program in an electronic assembly having information processing means and information storage means, said executable program code comprising instructions to direct a microprocessor of the electronic assembly to:

to replace directives inserted into a program, the directives corresponding to beacon and beacon functions, by a set of static data, beacon functions and verification functions to automatically integrate a set of valid executions represented by the static data, the beacon functions being used for calculating dynamically a representation of the execution; and

the verification functions being used to check the consistency of the static and dynamic data.

13. The computer executable storage medium of Claim 12 wherein the medium further comprises instructions to direct a microprocessor of the electronic assembly to use a control flow graph of the program to be protected to generate the static information used by the verification functions.

14. The computer executable storage medium of Claim 12 or 13 wherein a beacon is information which defines the characteristics of ~~the~~ a corresponding passage point and/or one or more other passage points.

15. The ~~microprocessor module~~ the computer executable storage medium of Claim 14 wherein the beacon is one of the following elements, a combination of several of them, or all of them:

an integer locating the beacon in the code to be protected;

a Boolean variable defining whether the beacon is the first or the last beacon;

a data structure characterizing, according to the value of a register or a given variable, all beacons through which passage will be forbidden ~~(using a verification function)~~ in the remaining execution;

a data structure comprising, according to the value of a register or a given variable, all beacons through which passage will be forced ~~(using a verification function)~~ in the remaining execution.

16. The ~~microprocessor module~~ computer readable storage medium of Claim 12 wherein the beacon function is called by the program ~~module~~ at each passage by a beacon and which will consist in storing dynamically in a shared memory various items of information concerning the beacon.

17. A method to secure at least one program designed to be integrated in an electronic assembly including information processing means and information storage means, comprising

inserting directives, corresponding to beacons and beacon functions, and intended for a pre-processor, into the code of the program;

causing the pre-processor to replace the directives in the code of the program by a set of static data, beacon functions and verification functions to automatically integrate a set of valid executions represented by the static data, the beacon functions being used for calculating dynamically a representation of the execution and the verification functions being used to check the consistency of the static and dynamic data.

Reasons for Allowance

2. The following is an examiner's statement of reasons for allowance: With respect to claim 17, the same reason for allowance applies as per canceled claim 2, as given in prior office action.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER S. MCCARTHY whose telephone number is (571)272-3651. The examiner can normally be reached on M-F, 9 - 5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Robert Beausoliel can be reached on (571)272-3645. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christopher S. McCarthy/
Primary Examiner, Art Unit 2113